Abstract of the Disclosure

In general, in one aspect, the invention relates to a method for accessing encrypted data by a client. The method includes receiving from the client by a server client information derived from a first secret wherein the client information is derived such that the server can not feasibly determine the first secret. The method also includes providing to the client by the server intermediate data, which is derived responsive to the received client information, a server secret, and possibly other information. The intermediate data is derived such that the client cannot feasibly determine the server secret. The method also includes authenticating the client by a device that stores encrypted secrets and is configured not to provide the encrypted secrets without authentication. After the authenticating step, the method also includes providing the encrypted secrets to the client. The encrypted secrets 5 are capable of being decrypted using a third secret that is derived from the intermediate data.

2031412_3